

# Equidistant subspace codes

Elisa Gorla and Alberto Ravagnani\*

Institut de Mathématiques  
Université de Neuchâtel  
Emile-Argand 11, CH-2000 Neuchâtel, Switzerland

## Abstract

In this paper we study equidistant subspace codes, i.e. subspace codes with the property that each two distinct codewords have the same distance. We provide an almost complete classification of such codes under the assumption that the cardinality of the ground field is large enough. More precisely, we prove that for most values of the parameters, an equidistant code of maximum cardinality is either a sunflower or the orthogonal of a sunflower. We also study equidistant codes with extremal parameters, and establish general properties of equidistant codes that are not sunflowers. Finally, we propose a systematic construction of equidistant codes based on our previous construction of partial spread codes, and provide an efficient decoding algorithm.

## Introduction

Network coding is a branch of information theory concerned with data transmission over noisy and lossy networks. A network is modeled by a directed acyclic multigraph, and information travels from one or multiple sources to multiple receivers through intermediate nodes. Network coding has several applications, e.g. peer-to-peer networking, distributed storage and patches distribution. In [1] it was proved that the information rate of a network communication may be improved employing coding at the nodes of the network, instead of simply routing the received inputs. In [16] it was shown that maximal information rate can be achieved in the multicast situation by allowing the intermediate nodes to perform linear combination of the inputs they receive, provided that the cardinality of the ground field is sufficiently large. Random linear network coding was introduced in [13], and a mathematical approach was proposed in [14] and [15], together with the definition of subspace code.

In this paper we study equidistant subspace codes, i.e., subspace codes with the property that the intersection of any pair of codewords has the same dimension. Equidistant subspace codes were shown to have relevant applications in distributed storage in [20]. In the same

---

2010 *Mathematics subject classification*: 11T71, 14G50, 94B60, 51E23, 15A21.

*Keywords*: network coding, equidistant subspace codes, sunflowers, spreads and partial spreads..

\*E-mails: [alberto.ravagnani@unine.ch](mailto:alberto.ravagnani@unine.ch), [elisa.gorla@unine.ch](mailto:elisa.gorla@unine.ch). The authors were partially supported by the Swiss National Science Foundation through grant no. 200021\_150207 and by the ESF COST Action IC1104.

paper, Etzion and Raviv identify two trivial families of equidistant codes, namely sunflowers and balls. A ball is a subspace code in the Grassmannian  $\mathcal{G}_q(k, n)$  of  $k$ -dimensional subspaces of  $\mathbb{F}_q^n$  with the property that all the elements of the code are contained in a fixed  $(k + 1)$ -dimensional subspace of  $\mathbb{F}_q^n$ . They proceed then to study the question of when an equidistant code belongs to one of the two families. Starting from the observation that the orthogonal of a ball is a sunflower, in this paper we study the question of when an equidistant code is either a sunflower or the orthogonal of a sunflower. One of our main results is a classification of equidistant subspace codes over fields of large enough cardinality: We prove that, for most choices of the parameters, an equidistant code of maximum cardinality is either a sunflower or the orthogonal of a sunflower. In addition, for most values of the parameters the two possibilities are mutually exclusive. We also study extremal equidistant codes, i.e. codes for which every two distinct codewords intersect in codimension one. We show that each such code is either a sunflower or the orthogonal of a sunflower, over fields of any size and for a code of any cardinality. We also establish general properties of equidistant codes that are not sunflowers. Finally, we give a systematic construction of asymptotically optimal equidistant codes based on the construction of partial spread codes from [12]. We then exploit the structure of our codes to design an efficient decoding algorithm for them and for their orthogonals.

The paper is organized as follows: In Section 1 we recall some definitions and results on subspace codes, equidistant codes, sunflowers and partial spreads. In Section 2 we study extremal equidistant codes, with the property that each two distinct elements intersect in codimension one. In Section 3 we give a classification of equidistant codes for most values of  $k, n$  and for  $q \gg 0$ . The classification is summarized in Theorem 27. In Section 4 we study equidistant codes that are not sunflowers. In Section 5 we give a systematic construction for sunflower codes, and we argue that their cardinality is asymptotically optimal. In Section 6 we show how to decode them efficiently and in Section 7 we explicitly describe their orthogonal codes and show how to decode them.

## 1 Preliminaries

We briefly recall the main definitions and results on subspace codes, equidistant codes, and partial spreads.

**Notation 1.** Throughout the paper  $q$  denotes a fixed prime power, and  $k, n$  two integers with  $1 \leq k < n$ . We denote by  $\mathcal{G}_q(k, n)$  the set of  $k$ -dimensional vector subspaces of  $\mathbb{F}_q^n$ .

**Definition 2.** The **subspace distance** between subspaces  $U, V \subseteq \mathbb{F}_q^n$  is defined by

$$d(U, V) := \dim(U) + \dim(V) - 2\dim(U \cap V).$$

A **subspace code** of constant dimension  $k$  is a subset  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  with  $|\mathcal{C}| \geq 2$ . The **minimum distance** of  $\mathcal{C}$  is  $d(\mathcal{C}) := \min\{d(U, V) : U, V \in \mathcal{C}, U \neq V\}$ . The code  $\mathcal{C}$  is **equidistant** if for all  $U, V \in \mathcal{C}$  with  $U \neq V$  we have  $d(U, V) = d(\mathcal{C})$ . An equidistant code  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  is  **$c$ -intersecting** if  $d(\mathcal{C}) = 2(k - c)$ .

Notice that equidistant  $c$ -intersecting codes exist only for  $n \geq 2k - c$ , since codes contain at least two codewords.

**Notation 3.** Given an integer  $0 \leq c \leq k - 1$ , we denote by  $e_q(k, n, c)$  the largest cardinality of an equidistant  $c$ -intersecting subspace code  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ .

**Definition 4.** An equidistant  $c$ -intersecting code  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  is **optimal** if  $|\mathcal{C}| = e_q(k, n, c)$ . A family of codes  $\mathcal{C}_q \subseteq \mathcal{G}_q(k, n)$  is **asymptotically optimal** if  $\lim_{q \rightarrow \infty} |\mathcal{C}_q|/e_q(k, n, c) = 1$ .

Partial spreads are a first example of equidistant subspace codes.

**Definition 5.** A **partial spread** in  $\mathcal{G}_q(k, n)$  is a subspace code  $\mathcal{S} \subseteq \mathcal{G}_q(k, n)$  with  $d(\mathcal{S}) = 2k$ .

The maximum cardinality of a partial spread  $\mathcal{S} \subseteq \mathcal{G}_q(k, n)$  is  $e_q(k, n, 0)$  by definition. A systematic construction for partial spreads and an efficient decoding algorithm are given in [12]. The cardinality of the codes from [12] meets the lower bound of the following well-known result (see e.g. [3]). It follows that the codes are asymptotically optimal.

**Theorem 6.** Let  $r$  denote the remainder obtained dividing  $n$  by  $k$ . We have

$$\frac{q^n - q^r}{q^k - 1} - q^r + 1 \leq e_q(k, n, 0) \leq \frac{q^n - q^r}{q^k - 1}.$$

**Remark 7.** The lower and upper bound of Theorem 6 agree when  $r = 0$ . In this case  $k$  divides  $n$  and the bound is always attained by codes that are called **spreads** (see [18] and the references within). When  $k$  does not divide  $n$ , deciding whether  $e_q(k, n, 0)$  may be equal to the upper bound for some values of  $q, k, n$  is an open problem. For some special values of  $q, k, n$  moreover, the lower bound of Theorem 6 can be improved, see e.g. [2] and [8].

Sunflowers are a main source of examples of equidistant codes.

**Definition 8.** A subspace code  $\mathcal{F} \subseteq \mathcal{G}_q(k, n)$  is a **sunflower** if there exists a subspace  $C \subset \mathbb{F}_q^n$  such that for all  $U, V \in \mathcal{F}$  with  $U \neq V$  we have  $U \cap V = C$ . The space  $C$  is called the **center** of the sunflower  $\mathcal{F}$ .

A sunflower  $\mathcal{F} \subseteq \mathcal{G}_q(k, n)$  with center  $C$  of dimension  $c$  is an equidistant  $c$ -intersecting subspace code with minimum distance  $2(k - c)$ . The connection between partial spreads and sunflowers is described in the following simple remark. The same observation appears in [9], Theorems 10 and 11.

**Remark 9.** Let  $\mathcal{F} \subseteq \mathcal{G}_q(k, n)$  be a sunflower with center  $C$  of dimension  $c$ , and let  $\varphi : \mathbb{F}_q^n/C \rightarrow \mathbb{F}_q^{n-c}$  be an isomorphism. Then the subspace code

$$\mathcal{S} := \{\varphi(U/C) : U \in \mathcal{F}\} \subseteq \mathcal{G}_q(k - c, n - c)$$

is a partial spread with  $|\mathcal{S}| = |\mathcal{F}|$ . Conversely, given an integer  $0 \leq c \leq k - 1$ , a partial spread  $\mathcal{S} \subseteq \mathcal{G}_q(k - c, n - c)$ , and a subspace  $C \subseteq \mathbb{F}_q^n$ , the subspace code  $\mathcal{F} := \{C \oplus U : U \in \mathcal{S}\} \subseteq \mathcal{G}_q(k, n)$  is a sunflower with center  $C$  and  $|\mathcal{F}| = |\mathcal{S}|$ .

By Remark 9 one easily obtains the

**Corollary 10.** For all  $0 \leq c \leq k - 1$  we have  $e_q(k, n, c) \geq e_q(k - c, n - c, 0)$ .

The following result shows that equidistant codes of large cardinality are sunflowers. The proof is based on a result by Deza on classical codes (see [6] and [7]), applied in the context of network coding by Etzion and Raviv.

**Theorem 11** ([9], Theorem 1). Let  $0 \leq c \leq k - 1$  be an integer, and let  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  be a  $c$ -intersecting equidistant code. Assume that

$$|\mathcal{C}| \geq ((q^k - q^c)/(q - 1))^2 + (q^k - q^c)/(q - 1) + 1.$$

Then  $\mathcal{C}$  is a sunflower.

**Remark 12.** Deza conjectured that any  $c$ -intersecting equidistant code  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  with  $|\mathcal{C}| > (q^{k+1} - 1)/(q - 1)$  is a sunflower (see [9], Conjecture 1). The conjecture was disproved in [9], Section 3.2, where the authors give an example of an equidistant code  $\mathcal{C} \subseteq \mathcal{G}_2(3, 6)$  of minimum distance 4 and cardinality 16, which is not a sunflower. The example was found by computer search.

We close this section with the definition of orthogonal and span of a code.

**Definition 13.** The **orthogonal** of a code  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  is  $\mathcal{C}^\perp := \{U^\perp : U \in \mathcal{C}\} \subseteq \mathcal{G}_q(n - k, n)$ , where  $U^\perp$  is the orthogonal of  $U$  with respect to the standard inner product of  $\mathbb{F}_q^n$ .

**Remark 14.** For any  $U, V \in \mathcal{G}_q(k, n)$  we have  $\dim(U^\perp \cap V^\perp) = n - 2k + \dim(U \cap V)$ . Hence  $d(\mathcal{C}) = d(\mathcal{C}^\perp)$  for any subspace code  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ . In particular, the orthogonal of a  $c$ -intersecting equidistant code  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  is a  $(n - 2k + c)$ -intersecting equidistant code (see also Theorem 13 and Theorem 14 of [9]). Notice that  $n - 2k + c \geq 0$ , since  $\mathcal{C}$  contains two distinct codewords. This proves that

$$e_q(k, n, c) = e_q(n - k, n, n - 2k + c)$$

for all  $0 \leq c \leq k - 1$ , and the orthogonal of an optimal equidistant code is an optimal equidistant code.

**Definition 15.** Let  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  be a subspace code. We define the **span** of  $\mathcal{C}$  as

$$\text{span}(\mathcal{C}) := \sum_{U \in \mathcal{C}} U \subseteq \mathbb{F}_q^n.$$

## 2 Extremal equidistant codes

In this section we study  $(k - 1)$ -intersecting codes in  $\mathcal{G}_q(k, n)$ . We call such codes **extremal**, since  $k - 1$  is the largest possible value of  $c$ , for given  $k$  and  $n$ . Notice that these codes are equidistant with minimum distance  $d = 2$ . In particular, the orthogonal of an extremal code is extremal. Our main result shows that every extremal equidistant code is either a sunflower, or the orthogonal of a sunflower. In Section 3 we establish a similar result for most choices of  $(k, n, c)$  and for  $q \gg 0$ .

**Proposition 16.** Let  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  be a  $c$ -intersecting equidistant code. The following are equivalent:

1.  $\mathcal{C}$  is a sunflower,
2.  $\dim \text{span}(\mathcal{C}^\perp) = n - c$ ,

3. for all  $A, B \in \mathcal{C}$  with  $A \neq B$  we have  $\text{span}(\mathcal{C}^\perp) = A^\perp + B^\perp$ .

*Proof.* Properties (2) and (3) are clearly equivalent. The code  $\mathcal{C}$  is a sunflower if and only if there exists  $C \subseteq \mathbb{F}_q^n$  with  $\dim(C) = c$  such that  $A \cap B = C$  for all  $A, B \in \mathcal{C}$  with  $A \neq B$ . The condition  $A \cap B = C$  is equivalent to  $A^\perp + B^\perp = C^\perp$ . Hence (1) and (3) are equivalent.  $\square$

The following may be regarded as classification of  $(k-1)$ -intersecting codes in  $\mathcal{G}_q(k, n)$ .

**Proposition 17.** Let  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  be a  $(k-1)$ -intersecting equidistant code. Then either  $\mathcal{C}$  is a sunflower, or  $\mathcal{C}^\perp$  is a sunflower.

*Proof.* If  $|\mathcal{C}| = 2$  the result is trivial. Assume  $|\mathcal{C}| \geq 3$  and that  $\mathcal{C}$  is not a sunflower. Let  $A, B \in \mathcal{C}$  with  $A \neq B$ . By Proposition 16 it suffices to show that  $\text{span}(\mathcal{C}) = A + B$ . Since  $\mathcal{C}$  is not a sunflower, there exists  $D \in \mathcal{C} \setminus \{A, B\}$  such that  $D \cap A \neq D \cap B$ . Since  $D \supseteq D \cap A + D \cap B$  and  $\dim(D \cap A + D \cap B) \geq \dim(D \cap A) + 1 = k$ , then  $D = D \cap A + D \cap B \subseteq A + B$ . For any  $E \in \mathcal{C} \setminus \{A, B, D\}$  we have  $E \supseteq E \cap A + E \cap B + E \cap D$ . Since  $\dim(A \cap B \cap D) < k-1$ , then  $E \cap A$ ,  $E \cap B$ , and  $E \cap D$  are not all equal. Hence  $\dim(E \cap A + E \cap B + E \cap D) \geq \dim(E \cap A) + 1 = k$  and  $E = E \cap A + E \cap B + E \cap D \subseteq A + B$ . Therefore  $\text{span}(\mathcal{C}) = A + B$ .  $\square$

As a corollary, we obtain an improvement of Theorem 12 and Corollary 1 of [9].

**Corollary 18.** Let  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  be a  $(k-1)$ -intersecting equidistant code. If  $\mathcal{C}$  is not a sunflower, then it is a subset of the set of  $k$ -dimensional subspaces of a given  $(k+1)$ -dimensional space. In particular, if  $|\mathcal{C}| > \begin{bmatrix} k+1 \\ k \end{bmatrix}$ , then  $\mathcal{C}$  is a sunflower.

*Proof.* If  $\mathcal{C}$  is not a sunflower, then by Proposition 17 the orthogonal code  $\mathcal{C}^\perp$  is a sunflower. By Proposition 16 this is equivalent to  $\dim \text{span}(\mathcal{C}) = k+1$ . Then all the codewords of  $\mathcal{C}$  are contained in a fixed  $(k+1)$ -dimensional space of  $\mathbb{F}_q^n$ . In particular, their number cannot exceed the number of  $k$ -dimensional subspaces of a  $(k+1)$ -dimensional space, a contradiction.  $\square$

**Remarks 19.** 1. Combining Theorem 6, Corollary 10, and Corollary 18, we have that if  $\mathcal{C}$  has maximum cardinality  $e_q(k, n, k-1)$  and  $n \gg 0$ , then  $\mathcal{C}$  is a sunflower.

2. As observed in [9], the bound of Corollary 18 is sharp for any  $k, n$ . In fact, let  $\mathcal{C}$  be the set of  $k$ -dimensional subspaces of a fixed  $(k+1)$ -dimensional space of  $\mathbb{F}_q^n$ .  $\mathcal{C}$  is an equidimensional  $(k-1)$ -intersecting code of cardinality  $\begin{bmatrix} k+1 \\ k \end{bmatrix}$  which is not a sunflower.

### 3 A classification of equidistant codes

In this section we provide a classification of optimal equidistant codes for most values of the parameters. More precisely we prove that, for  $q \gg 0$  and for most values of  $k$  and  $n$ , every optimal equidistant code is either a sunflower or the orthogonal of a sunflower. We start by studying the case when  $k$  is small with respect to  $n$ .

**Proposition 20.** Let  $q \gg 0$  and  $n \geq 3k - 1$ . Then

$$e_q(k, n, c) = e_q(k - c, n - c, 0).$$

Moreover, any  $c$ -intersecting equidistant code  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  of cardinality  $e_q(k, n, c)$  is a sunflower.

*Proof.* Let  $0 \leq r \leq k - c - 1$  denote the remainder obtained dividing  $n - c$  by  $k - c$ . Since  $n > 3k - 2 \geq 2k - 1$ , we have  $r \leq k - 1 < n - k$ . Therefore

$$\lim_{q \rightarrow \infty} \frac{\frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1}{q^{n-k}} = 1.$$

On the other hand

$$\lim_{q \rightarrow \infty} \frac{\left(\frac{q^k - q^c}{q - 1}\right)^2 + \frac{q^k - q^c}{q - 1} + 1}{q^{2k-2}} = 1.$$

Since  $k < (n + 2)/3$  we have  $n - k > 2k - 2$ . Hence

$$\lim_{q \rightarrow \infty} \frac{\frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1 - \left[\left(\frac{q^k - q^c}{q - 1}\right)^2 + \frac{q^k - q^c}{q - 1} + 1\right]}{q^{n-k}} = 1.$$

In particular, for  $q \gg 0$  we have

$$\frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1 \geq \left(\frac{q^k - q^c}{q - 1}\right)^2 + \frac{q^k - q^c}{q - 1} + 1.$$

By Theorem 6 and Corollary 10 we have

$$|\mathcal{C}| \geq \frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1 \geq \left(\frac{q^k - q^c}{q - 1}\right)^2 + \frac{q^k - q^c}{q - 1} + 1.$$

Theorem 11 implies that  $\mathcal{C}$  is a sunflower. Hence by Remark 9 we have  $e_q(k, n, c) = e_q(k - c, n - c, 0)$ .  $\square$

For completeness we also examine the case when  $n$  is small with respect to  $k$ .

**Proposition 21.** Let  $q \gg 0$  and  $n \leq (3k + 1)/2$ . Then

$$e_q(k, n, c) = e_q(k - c, 2k - c, 0).$$

Moreover, every  $c$ -intersecting equidistant code  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  of cardinality  $e_q(k, n, c)$  is of the form  $\mathcal{S}^\perp$ , where  $\mathcal{S}$  is a sunflower.

*Proof.* By Remark 14 we have  $e_q(k, n, c) = e_q(n - k, n, n - 2k + c)$ . Since  $n \geq 3(n - k) - 1$ , the thesis follows from Proposition 20.  $\square$

Proposition 20 and Proposition 21 imply that for  $n \leq (3k + 1)/2$  or for  $n \geq 3k - 1$  and  $q \gg 0$ , every equidistant code of maximum cardinality  $e_q(k, n, c)$  is either a sunflower, or the orthogonal of a sunflower. We now show that these families are almost always disjoint.

**Lemma 22.** Let  $\mathcal{S} \subseteq \mathcal{G}_q(k, n)$  be a sunflower with center  $C$  of dimension  $0 \leq c \leq k - 1$  and  $\text{span}(\mathcal{S}) = \mathbb{F}_q^n$ . Assume that  $n > 2k - c$ . Then  $\mathcal{S}^\perp$  is not a sunflower.

*Proof.* By contradiction, assume that  $\mathcal{S}^\perp \subseteq \mathcal{G}_q(n - k, n)$  is a sunflower with center  $D$ . By Remark 14  $\dim(D) = n - 2k + c > 0$ . Moreover,  $D \subseteq U^\perp$  for all  $U \in \mathcal{S}$ , i.e.,  $U \subseteq D^\perp$  for all  $U \in \mathcal{S}$ . Then  $\mathbb{F}_q^n = \text{span}(\mathcal{S}) \subseteq D^\perp$ , which contradicts the assumption that  $D \neq 0$ .  $\square$

Remark 14 and Lemma 22 allow us to construct a family of equidistant codes which are not sunflowers and have maximum cardinality for their parameters.

**Example 23.** Let  $n = \ell k$ ,  $\ell > 2$ . Let  $\mathcal{S} \subseteq \mathcal{G}_q(k, \ell k)$  be a spread. Then  $\mathcal{S}^\perp$  is an optimal equidistant code which is not a sunflower by Lemma 22. We have

$$|\mathcal{S}^\perp| = |\mathcal{S}| = e_q(k, \ell k, 0) = e_q((\ell - 1)k, \ell k, (\ell - 2)k),$$

where the last equality follows from Remark 14.

Setting  $k = 1$  we recover two well-known examples of equidistant codes:  $\mathcal{S}$  is the set of lines in  $\mathbb{F}_q^\ell$  and  $\mathcal{S}^\perp$  is the set of  $(\ell - 1)$ -dimensional subspaces of  $\mathbb{F}_q^\ell$ .

Now we prove that a  $c$ -intersecting sunflower  $\mathcal{S} \subseteq \mathcal{G}_q(k, n)$  with maximum cardinality  $e_q(k, n, c)$  is never contained in a proper subspace of  $\mathbb{F}_q^n$ .

**Proposition 24.** Let  $\mathcal{S} \subseteq \mathcal{G}_q(k, n)$  be a sunflower with center of dimension  $0 \leq c \leq k - 1$ . Let  $r$  denote the remainder obtained dividing  $n - c$  by  $k - c$ . If

$$|\mathcal{S}| \geq \frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1,$$

then  $\text{span}(\mathcal{S}) = \mathbb{F}_q^n$ . In particular, if  $|\mathcal{S}| = e_q(k, n, c)$  then  $\text{span}(\mathcal{S}) = \mathbb{F}_q^n$ .

*Proof.* Since  $\mathcal{S}$  is a sunflower with center of dimension  $c$ , we have

$$\begin{aligned} \left| \bigcup_{V \in \mathcal{S}} V \right| &= q^c + |\mathcal{S}|(q^k - q^c) \\ &\geq q^c + q^c(q^{k-c} - 1) \left( \frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1 \right) \\ &= q^n + q^k - q^{k+r} \\ &\geq q^n + q^k - q^{2k-c-1}. \end{aligned}$$

Since  $|\mathcal{S}| \geq 2$ , then  $n \geq 2k - c$ , hence  $q^n + q^k - q^{2k-c-1} \geq q^n + q^k - q^{n-1} > q^{n-1}$ . Therefore  $\mathcal{S}$  cannot be contained in a proper subspace of  $\mathbb{F}_q^n$ . The second part of the statement follows from Corollary 10 and Theorem 6.  $\square$

**Corollary 25.** Let  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  be a  $c$ -intersecting equidistant code with  $|\mathcal{C}| = e_q(k, n, c)$ . Then  $\mathcal{C}$  and  $\mathcal{C}^\perp$  are both sunflowers if and only if  $n = 2k$  and both  $\mathcal{C}$  and  $\mathcal{C}^\perp$  are spreads.

*Proof.* Assume that both  $\mathcal{C}$  and  $\mathcal{C}^\perp$  are sunflowers. By Remark 14 the center of  $\mathcal{C}^\perp$  has dimension  $c' = n - 2k + c \geq 0$ . Since  $|\mathcal{C}| = e_q(k, n, c)$ , Proposition 24 and Lemma 22 applied to  $\mathcal{C}$  give  $c' = 0$ . In particular,  $\mathcal{C}^\perp$  is a partial spread. Since  $\mathcal{C}$  is optimal, then  $\mathcal{C}^\perp$  is optimal by Remark 14. By Proposition 24 and Lemma 22,  $c = n - 2(n - k) + c' = 0$ . Hence  $n = 2k$  and  $\mathcal{C}$  is a partial spread. Since  $n = 2k$  and  $\mathcal{C}$  and  $\mathcal{C}^\perp$  have maximum cardinality, they are spreads.  $\square$

Hence when  $n = 2k$  and  $c = 0$ , every 0-intersecting equidistant code  $\mathcal{C} \subseteq \mathcal{G}_q(k, 2k)$  of maximum cardinality is a spread, and its orthogonal is again a spread with the same parameters. Therefore every equidistant code of maximum cardinality is a sunflower, as well as its orthogonal.

For  $n = 2k$  and  $c > 0$ ,  $e_q(k, 2k, c) \geq e_q(k - c, 2k - c, 0)$  by Corollary 10, and the two quantities do not always agree, e.g.

$$e_q(3, 6, 1) > e_q(2, 5, 0),$$

as shown in the next example. Moreover, for any  $k, c$  for which  $e_q(k, 2k, c) = e_q(k - c, 2k - c, 0)$ , let  $\mathcal{C} \subseteq \mathcal{G}_q(k, 2k)$  be a  $c$ -intersecting sunflower of cardinality  $e_q(k, 2k, c)$ . Then by Corollary 25 we also have a  $c$ -intersecting equidistant code  $\mathcal{C}^\perp \subseteq \mathcal{G}_q(k, 2k)$  of maximum cardinality which is not a sunflower. Hence for any  $k, c$  we have  $c$ -intersecting equidistant codes  $\mathcal{C} \subseteq \mathcal{G}(k, 2k)$  of maximum cardinality which are not sunflowers, but we may not always have sunflower codes of the same cardinality.

In addition, it may be possible to also have an equidistant code  $\mathcal{C} \subseteq \mathcal{G}_q(k, 2k)$  of cardinality  $e_q(k, 2k, c)$  such that neither  $\mathcal{C}$  nor  $\mathcal{C}^\perp$  are sunflowers. This is the case of the following example.

**Example 26** ([4], Example 1.2). The hyperbolic Klein set  $\mathcal{C} \subseteq \mathcal{G}(3, 6)$  is an equidistant code with  $c = 1$  and  $|\mathcal{C}| = q^3 + q^2 + q + 1$ .  $\mathcal{C}$  is not a sunflower, nor the orthogonal of a sunflower, since the largest possible cardinality of a sunflower with  $k = 3, n = 6, c = 1$  is

$$e_q(2, 5, 0) \leq \frac{q^5 - q}{q^2 - 1} = q^3 + q < |\mathcal{C}| = |\mathcal{C}^\perp|,$$

where the inequality follows from Theorem 6. In particular,  $e_q(3, 6, 1) > e_q(2, 5, 0)$ .

Combining Propositions 17, 20, 21, 24, and Corollary 25 one easily obtains the following classification of equidistant codes of maximum cardinality.

**Theorem 27.** Let  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  be a  $c$ -intersecting equidistant code with  $|\mathcal{C}| = e_q(k, n, c)$ . Assume that one of the following conditions holds:

- $c \in \{0, k - 1, 2k - n\}$ ,
- $n \leq (3k + 1)/2$  and  $q \gg 0$ ,
- $n \geq 3k + 1$  and  $q \gg 0$ .

Then either  $\mathcal{C}$  is a sunflower or  $\mathcal{C}^\perp$  is a sunflower, and the two are mutually exclusive unless  $c = 0$  and  $n = 2k$ .

Notice that  $n \gg k$  is the relevant practical situation within network coding. Moreover, one needs to assume  $q \gg 0$  in order to have a solution to the network coding problem (see [19], Chapter 1 for details).



## 4 Other properties of equidistant codes

We devote this section to equidistant codes that are not sunflowers. The property of having a center characterizes sunflowers among equidistant codes.

**Definition 28.** Let  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  be a  $c$ -intersecting equidistant code,  $0 \leq c \leq k - 1$ . The **set of centers** of  $\mathcal{C}$  is  $T(\mathcal{C}) := \{U \cap V : U, V \in \mathcal{C}, U \neq V\}$ , and the **number of centers** of  $\mathcal{C}$  is  $t(\mathcal{C}) := |T(\mathcal{C})|$ . The **set of petals** attached to a center  $A \in T(\mathcal{C})$  is  $\mathcal{P}(A) := \{U \in \mathcal{C} : A \subseteq U\}$ .

In the next proposition we show that equidistant codes that have many codewords are either sunflowers, or they have a large number of centers.

**Proposition 29.** Let  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  be an  $c$ -intersecting equidistant code,  $0 \leq c \leq k - 1$ . One of the following properties holds:

1.  $\mathcal{C}$  is a sunflower, or
2.  $t(\mathcal{C}) \geq |\mathcal{C}| \frac{q^c - q^{c-1}}{q^k - q^{c-1}}$ .

*Proof.* If  $\mathcal{C}$  is not a sunflower, then  $t := t(\mathcal{C}) \geq 2$ . Choose an enumeration  $T(\mathcal{C}) = \{A_1, \dots, A_t\}$ . Since  $\mathcal{C} = \bigcup_{i=1}^t \mathcal{P}(A_i)$ , we have

$$|\mathcal{C}| \leq \sum_{i=1}^t |\mathcal{P}(A_i)|. \quad (1)$$

For any  $i \in \{1, \dots, t\}$ ,  $\mathcal{P}(A_i)$  is a sunflower with  $c$ -dimensional center  $A_i$ , minimum distance  $2(k - c)$ , and cardinality  $s_i := |\mathcal{P}(A_i)|$ . If  $V \in \mathcal{C} \setminus \mathcal{P}(A_i)$ , then

$$|V| \geq \left| V \cap \bigcup_{U \in \mathcal{P}(A_i)} U \right| = \sum_{U \in \mathcal{P}(A_i)} |V \cap U| - (s_i - 1)|V \cap A_i| = s_i|A_i| - (s_i - 1)|V \cap A_i|$$

hence  $q^k \geq s_i q^c - (s_i - 1)q^{c-1} = s_i(q^c - q^{c-1}) + q^{c-1}$ . Therefore we have shown that

$$|\mathcal{P}(A_i)| \leq \frac{q^k - q^{c-1}}{q^c - q^{c-1}}$$

for all  $1 \leq i \leq t$ , and the thesis follows by (1).  $\square$

In particular, for a code with maximum cardinality which is not a sunflower, we can give the following asymptotic estimate of the number of centers as  $q$  grows.

**Corollary 30.** Let  $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$  be a  $c$ -intersecting equidistant code. Assume that  $|\mathcal{C}| = e_q(k, n, c)$  and that  $\mathcal{C}$  is not a sunflower. Denote by  $r$  the remainder of the division of  $n - c$  by  $k - c$ . Then

$$t(\mathcal{C}) \geq e_q(k, n, c) \frac{q^c - q^{c-1}}{q^k - q^{c-1}} \geq \left( \frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1 \right) \frac{q^c - q^{c-1}}{q^k - q^{c-1}}.$$

In particular,  $\lim_{q \rightarrow \infty} t(\mathcal{C}) q^{-(n-2k+c)} \in [1, +\infty]$ .

*Proof.* The inequality follows by Proposition 29, Corollary 10, and Theorem 6. Hence

$$\lim_{q \rightarrow \infty} t(\mathcal{C})q^{-(n-2k+c)} \geq \lim_{q \rightarrow \infty} \left( \frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1 \right) \frac{q^c - q^{c-1}}{q^k - q^{c-1}} q^{-(n-2k+c)} = 1,$$

as claimed.  $\square$

The orthogonal of a sunflower is often an example of an optimal code with a large number of centers.

**Example 31.** Let  $0 < c \leq k - 1$ ,  $\mathcal{S} \subset \mathcal{G}_q(n - k, n)$  be a sunflower of maximum cardinality with  $(n - 2k + c)$ -dimensional center. Let  $\mathcal{C} = \mathcal{S}^\perp \subset \mathcal{G}_q(k, n)$ , then  $\mathcal{C}$  is  $c$ -intersecting and  $|\mathcal{C}| = |\mathcal{S}|$ .  $\mathcal{C}$  is not a sunflower by Corollary 25 and it has

$$t(\mathcal{C}) = \binom{|\mathcal{C}|}{2}.$$

In fact, for any  $A, B, D \in \mathcal{S}$  pairwise distinct one has

$$\dim(A + B)^\perp = n - 2k + c > n - 3k + 2c = \dim(A + B + D)^\perp,$$

hence

$$A^\perp \cap B^\perp \neq A^\perp \cap B^\perp \cap D^\perp.$$

In particular, there exist no distinct  $A^\perp, B^\perp, D^\perp \in \mathcal{C}$  such that  $A^\perp \cap D^\perp = B^\perp \cap D^\perp$ . Similarly one shows that there exist no distinct  $A^\perp, B^\perp, D^\perp, E^\perp \in \mathcal{C}$  such that  $A^\perp \cap D^\perp = B^\perp \cap E^\perp$ .

## 5 A systematic construction of sunflower codes

In this section we modify the construction of partial spreads proposed in [12] to systematically produce sunflower codes for any choice of  $k, n, c$ . We are motivated by Proposition 20 where we show that every equidistant code of maximum cardinality is a sunflower, provided that  $q \gg 0$  and  $n \geq 3k - 1$ . An efficient decoding algorithm is given in Section 6.

**Notation 32.** Denote by  $I_m$  an identity matrix of size  $m \times m$ , by  $0_m$  a zero matrix of size  $m \times m$ , and by  $0_{m \times \ell}$  a zero matrix of size  $m \times \ell$ .

**Definition 33.** Let  $p \in \mathbb{F}_q[x]$  be an irreducible monic polynomial of degree  $s \geq 1$ . Write  $p(x) = x^s + \sum_{i=0}^{s-1} p_i x^i$ . The **companion matrix** of  $p$  is the  $s \times s$  matrix

$$M(p) := \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{s-1} \end{bmatrix}.$$

The construction of sunflower codes which we propose is based on companion matrices of polynomials. It extends the constructions of [18] and [12].

**Theorem 34.** Let  $1 \leq k < n$  and  $\min\{0, 2k - n\} \leq c \leq k - 1$  be integers. Write  $n - c = h(k - c) + r$ , with  $0 \leq r \leq k - c - 1$ ,  $h \geq 2$ . Choose irreducible monic polynomials  $p, p' \in \mathbb{F}_q[x]$  of degree  $k - c$  and  $k - c + r$ , respectively. Set  $P := M(p)$  and  $P' := M(p')$ . For  $1 \leq i \leq h - 1$  let  $\mathcal{M}_i(p, p')$  be the set of  $k \times n$  matrices of the form

$$\begin{bmatrix} I_c & 0_{c \times (k-c)} & \cdots & \cdots & \cdots & \cdots & \cdots & 0_{c \times (k-c)} & 0_{c \times (k-c+r)} \\ 0_{(k-c) \times c} & 0_{k-c} & \cdots & 0_{k-c} & I_{k-c} & A_{i+1} & \cdots & A_{h-1} & A_{[k-c]} \end{bmatrix},$$

where we have  $i - 2$  consecutive copies of  $0_{k-c}$ , the matrices  $A_{i+1}, \dots, A_{h-1} \in \mathbb{F}_q[P]$ ,  $A \in \mathbb{F}_q[P']$ , and  $A_{[k-c]}$  denotes the last  $k - c$  rows of  $A$ . The set

$$\begin{aligned} \mathcal{C} := & \bigcup_{i=1}^{h-1} \{\text{rowsp}(M) : M \in \mathcal{M}_i(p, p')\} \\ & \cup \left\{ \text{rowsp} \begin{bmatrix} I_c & 0_{c \times (k-c)} & \cdots & 0_{c \times (k-c)} & 0_{c \times (k-c+r)} & 0_{c \times (k-c)} \\ 0_{(k-c) \times c} & 0_{k-c} & \cdots & 0_{k-c} & 0_{(k-c) \times (k-c+r)} & I_{k-c} \end{bmatrix} \right\} \end{aligned}$$

is a sunflower in  $\mathcal{G}_q(k, n)$  of cardinality

$$|\mathcal{C}| = \frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1.$$

*Proof.* Let  $C := \{v \in \mathbb{F}_q^n : v_i = 0 \text{ for } i > c\}$ . To simplify the notation, let  $B$  denote the matrix

$$\begin{bmatrix} I_c & 0_{c \times k-c} & \cdots & 0_{c \times k-c} & 0_{c \times k-c+r} & 0_{c \times k-c} \\ 0_{k-c \times c} & 0_{k-c} & \cdots & 0_{k-c} & 0_{k-c \times k-c+r} & I_{k-c} \end{bmatrix}.$$

Given a matrix  $M \in \mathcal{M}_i(p, p') \cup \{B\}$ , let  $\overline{M}$  be the matrix obtained from  $M$  by deleting the first  $c$  rows. We identify  $\mathbb{F}_q^{n-c}$  with  $\{v \in \mathbb{F}_q^n : v_i = 0 \text{ for } i = 1, \dots, c\}$ , so that  $\mathbb{F}_q^n = C \oplus \mathbb{F}_q^{n-c}$ . For any  $M \in \mathcal{M}_i(p, p') \cup \{B\}$  we have  $\text{rowsp}(\overline{M}) \subseteq \mathbb{F}_q^{n-c}$ . It follows

$$\mathcal{C} = \{C \oplus \text{rowsp}(\overline{M}) : M \in \mathcal{M}_i(p, p') \cup \{B\}\}.$$

By [12], Theorem 13 and Proposition 17, the set  $\{\text{rowsp}(\overline{M}) : M \in \mathcal{M}_i(p, p') \cup \{B\}\}$  is a partial spread in  $\mathcal{G}_q(k - c, n - c)$  of cardinality  $(q^{n-c} - q^r)/(q^{k-c} - 1) - q^r + 1$ . The theorem now follows from Remark 9.  $\square$

**Notation 35.** We denote the sunflower of Theorem 34 by  $\mathcal{F}_q(k, n, c, p, p')$ , and we call it a **sunflower code**. If  $h = 2$ , then the construction does not depend on  $p$  and we denote the code by  $\mathcal{F}_q(k, n, c, p')$ . In the sequel we will work with a fixed integer  $0 \leq c \leq k - 1$  and with fixed polynomials  $p$  and  $p'$  as in Theorem 34.

**Example 36.** Let  $q = 2$ ,  $c = 1$ ,  $k = 3$  and  $n = 6$ . Let  $p' := x^3 + x + 1 \in \mathbb{F}_2[x]$ . The companion matrix of  $p'$  is

$$P' = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

A codeword of  $\mathcal{F}_q(3, 6, 1, p')$  is either the space generated by the rows of the matrix

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

or the space generated by the rows of a matrix of the form

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & & I_2 & & A_{(2)} & \\ 0 & & & & & \end{bmatrix},$$

where  $I_2$  is the  $2 \times 2$  identity matrix, and  $A_{(2)}$  denotes the last two rows of a matrix  $A \in \mathbb{F}_2[P']$ . One can easily check that  $|\mathcal{F}_2(3, 6, 1, p, p')| = 2^3 + 1$ .

For most choices of the parameters, sunflower codes have asymptotically optimal cardinality, as the following result shows.

**Proposition 37.** Let  $n \geq 3k - 1$ , and let  $r$  denote the remainder obtained dividing  $n - c$  by  $k - c$ . For  $q \gg 0$  we have

$$e_q(k, n, c) - |\mathcal{F}_q(k, n, c, p, p')| \leq q^r - 1.$$

In particular,

$$\lim_{q \rightarrow \infty} \frac{|\mathcal{F}_q(k, n, c, p, p')|}{e_q(k, n, c)} = 1.$$

*Proof.* By Proposition 20 and Theorem 6 we have  $e_q(k, n, c) = e_q(k - c, n - c, 0) \leq \frac{q^{n-c} - q^r}{q^{k-c} - 1}$ . By Theorem 34 it follows that

$$e_q(k, n, c) - |\mathcal{F}_q(k, n, c, p, p')| \leq \frac{q^{n-c} - q^r}{q^{k-c} - 1} - |\mathcal{F}_q(k, n, c, p, p')| = q^r - 1.$$

If in addition  $n \geq 3k - 1$ , by Proposition 20 the integers  $q, k, n, c$  satisfy condition  $(*)$  for  $q \gg 0$ . By definition  $|\mathcal{F}_q(k, n, c, p, p')| \leq e_q(k, n, c)$ . It follows that for  $q \gg 0$

$$e_q(k, n, c) - q^r + 1 \leq |\mathcal{F}_q(k, n, c, p, p')| \leq e_q(k, n, c). \quad (2)$$

Since  $r \leq k - c - 1 \leq k - 1 < n - k$ , the second part of the thesis follows taking the limit of (2).  $\square$

## 6 Decoding sunflowers codes

In this section we provide an efficient decoding algorithm for the sunflower codes that we constructed in Section 5, by reducing decoding sunflower codes to decoding partial spread codes.

**Definition 38.** Let  $1 \leq t \leq n$  be an integer. A matrix  $M$  of size  $t \times n$  over  $\mathbb{F}_q$  is said to be in **reduced row-echelon form** if:

1.  $M$  is in row-echelon form;
2. the first non-zero entry of each row of  $M$  is a 1, and it is the only non-zero entry in its column.

**Remark 39.** It is well-known that for any  $1 \leq t \leq n$  and any  $t$ -dimensional  $\mathbb{F}_q$ -subspace  $X \subseteq \mathbb{F}_q^n$ , there exists a unique  $t \times n$  matrix in reduced row-echelon form and with entries in  $\mathbb{F}_q$  such that  $\text{rowsp}(M) = X$ .

**Notation 40.** We denote the matrix  $M$  of Remark 39 by  $\text{RRE}(X)$ .

The decoding algorithm for sunflower codes that we propose is based on the following result.

**Theorem 41.** Let  $V \in \mathcal{F}_q(k, n, c, p, p')$ ,  $V = \text{rowsp}(M)$  where  $M$  is as in Theorem 34:

$$M = \text{rowsp} \begin{bmatrix} I_c & 0_{c \times n-c} \\ 0_{k-c \times c} & B \end{bmatrix},$$

with  $B$  of size  $(k-c) \times (n-c)$ . Let  $X \subseteq \mathbb{F}_q^n$  be a subspace of dimension  $1 \leq t \leq k$ . Assume that  $X$  decodes to  $V$ , i.e.,  $d(V, X) < k-c$ . Then:

1.  $t > c$  and there exist matrices  $X_1, X_2, X_3$  of size  $c \times c$ ,  $c \times (n-c)$  and  $(t-c) \times (n-c)$  respectively, such that

$$\text{RRE}(X) = \begin{bmatrix} X_1 & X_2 \\ 0_{(t-c) \times c} & X_3 \end{bmatrix}.$$

2.  $d(\text{rowsp}(B), \text{rowsp}(X_3)) < k-c$ .

*Proof.* The condition  $d(V, X) < k-c$  is equivalent to  $\dim(V+X) < k + (t-c)/2$ . In particular we have  $k = \dim(V) \leq \dim(V+X) < k + (t-c)/2$ , and so  $t > c$ . Notice moreover that by Definition 38 the  $i$ -th row of any matrix in reduced row-echelon form contains at least  $i-1$  zeros. As a consequence,

$$\text{RRE}(X) = \begin{bmatrix} X_1 & X_2 \\ 0_{t-c \times c} & X_3 \end{bmatrix}$$

for some matrices  $X_1, X_2$  and  $X_3$  of size  $c \times c$ ,  $c \times (n-c)$  and  $(t-c) \times (n-c)$  respectively. To simplify the notation, we omit the size of the zero matrices in the sequel. The condition  $\dim(V+X) < k + (t-c)/2$  may be written as

$$\text{rk} \begin{bmatrix} I_c & 0 \\ 0 & B \\ X_1 & X_2 \\ 0 & X_3 \end{bmatrix} < k + (t-c)/2.$$

Hence we have

$$\text{rk} \begin{bmatrix} B \\ X_3 \end{bmatrix} = \text{rk} \begin{bmatrix} I_c & 0 \\ 0 & B \\ 0 & X_3 \end{bmatrix} - c \leq \text{rk} \begin{bmatrix} I_c & 0 \\ 0 & B \\ X_1 & X_2 \\ 0 & X_3 \end{bmatrix} - c < (k-c) + (t-c)/2.$$

Since  $\dim(X) = t$ , we have  $\text{rk}(X_3) = t - c$ . It follows that

$$\begin{aligned} d(\text{rowsp}(B), \text{rowsp}(X_3)) &= 2\text{rk} \begin{bmatrix} B \\ X_3 \end{bmatrix} - \text{rk}(B) - \text{rk}(X_3) \\ &< 2(k - c) + t - c - (k - c) - (t - c) \\ &= k - c, \end{aligned}$$

as claimed.  $\square$

Theorem 41 provides in particular the following efficient algorithm to decode a sunflower code.

**Algorithm 42** (Decoding a  $\mathcal{F}_q(k, n, c, p, p')$  code).

- **Input:** A decodable subspace  $X \subseteq \mathbb{F}_q^n$  of dimension  $t \leq k$ .
  - **Output:** The unique  $V \in \mathcal{F}_q(k, n, c, p, p')$  such that  $d(V, X) < k - c$ , given as a matrix in row-reduced echelon form whose row space is  $V$ .
1. Compute  $M := \text{RRE}(X)$ .
  2. Delete from  $M$  the first  $c$  rows and columns, obtaining a matrix  $\overline{M}$  of size  $k - c \times n - c$ .
  3. Apply partial spread decoding to  $\text{rowsp}(\overline{M})$  as described in [12], Section 5, and obtain a matrix  $N$  of size  $k - c \times n - c$ .
  4. The result is  $V = \text{rowsp} \begin{bmatrix} I_c & 0 \\ 0 & N \end{bmatrix}$ .

**Remark 43.** For any decodable subspace,  $t > c$  by Theorem 41. The assumption  $t \leq k$  is not restrictive from the following point of view: The receiver may collect incoming vectors until the received subspace has dimension  $k$ , and then attempt to decode the collected data. We also notice that the computation of  $\text{RRE}(X)$  has a low computational cost. Indeed, the receiver obtains the subspace  $V$  as the span of incoming vectors, i.e., as the row space of a matrix. The reduced row-echelon form of such matrix may be computed by Gaussian elimination.

## 7 The orthogonal of a sunflower code

By Proposition 24 and Lemma 22, the orthogonals of sunflower codes of Theorem 34 are equidistant codes that are not sunflowers. Moreover, they are asymptotically optimal equidistant codes for sufficiently large parameters (Remark 14 and Theorem 27). We can easily write them as rowspaces of matrices, as we show in this section. We will need the following preliminary lemma, whose proof is left to the reader.

**Lemma 44.** Let  $N$  be a  $t \times (n - t)$  matrix over  $\mathbb{F}_q$ . We have

$$\text{rowsp} \left( \begin{bmatrix} I_t & N \end{bmatrix} \right)^\perp = \text{rowsp} \left( \begin{bmatrix} -N^t & I_{(n-t) \times (n-t)} \end{bmatrix} \right).$$

**Remark 45.** Lemma 44 allows us to construct the orthogonal of a vector space  $V$  given as the rowspan of a full-rank matrix  $M$  in reduced row-echelon form. Indeed, if  $M$  is such a matrix of size, say,  $t \times n$ , then there exists a permutation  $\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  such that  $M^\pi$  has the form  $[I_t \ N]$ , where  $M^\pi$  is the matrix whose  $\pi(i)$ -th columns is the  $i$ -th column of  $M$ . By Lemma 44 we have  $V^\perp = \text{rowsp} \left( \begin{bmatrix} -N^t & I_{(n-t) \times (n-t)} \end{bmatrix}^{\pi^{-1}} \right)$ .

**Remark 46.** Remark 45 allows us to describe in matrix form the orthogonal of a sunflower code  $\mathcal{C} = \mathcal{F}_q(k, n, c, p, p')$ . Indeed, following the notation of Theorem 34, the orthogonal of the rowspan of the matrix

$$\begin{bmatrix} I_c & 0_{c \times (k-c)} & \cdots & \cdots & \cdots & \cdots & \cdots & 0_{c \times (k-c)} & 0_{c \times (k-c+r)} \\ 0_{(k-c) \times c} & 0_{k-c} & \cdots & 0_{k-c} & I_{k-c} & A_{i+1} & \cdots & A_{h-1} & A_{[k-c]} \end{bmatrix}$$

is the rowspan of the matrix

$$\begin{bmatrix} 0_{(k-c) \times c} & & & & 0_{k-c} & \cdots & \cdots & \cdots & \cdots \\ \vdots & & I_{(i-1)(k-c)} & & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & & & & 0_{k-c} & \vdots & \vdots & \vdots & \vdots \\ \vdots & 0_{k-c} & \cdots & 0_{k-c} & -A_{i+1}^t & & & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & & I_{n-k-(i-1)(k-c)} & & \\ \vdots & \vdots & \vdots & \vdots & -A_{h-1}^t & & & & \\ 0_{(k-c+r) \times c} & 0_{(k-c+r) \times (k-c)} & \cdots & \cdots & -A_{[k-c]}^t & & & & \end{bmatrix}.$$

Algorithm 42 and Remark 45 can also be combined to efficiently decode the orthogonal of a sunflower code.

**Remark 47.** Let  $\mathcal{C} = \mathcal{F}_q(k, n, c, p, p')$  be a sunflower code, and let  $X \subseteq \mathbb{F}_q^k$  be a received  $t$ -dimensional space. Since  $d(\mathcal{C}) = d(\mathcal{C}^\perp)$  and  $d(X, V^\perp) = d(X^\perp, V)$  for all  $V \in \mathcal{C}$ , the space  $X$  decodes to  $V^\perp$  in  $\mathcal{C}^\perp$  if and only if  $X^\perp$  decodes to  $V$  in  $\mathcal{C}$ . This gives the following Algorithm 48 to decode the orthogonal of a sunflower code.

**Algorithm 48** (Decoding a  $\mathcal{F}_q(k, n, c, p, p')^\perp$  code).

- **Input:** A decodable subspace  $X \subseteq \mathbb{F}_q^n$  of dimension  $t \geq n - k$ .
  - **Output:** The unique  $V \in \mathcal{F}_q(k, n, c, p, p')$  such that  $d(V^\perp, X) < k - c$ , given as a matrix whose rowspan is  $V$ .
1. Compute  $L := \text{RRE}(X)$ .
  2. Use Remark 45 to construct a matrix  $L'$  such that  $\text{rowsp}(L') = X^\perp$ .
  3. Compute the reduced row-echelon form, say  $M$ , of  $L'$ . Since  $t \geq n - k$ ,  $M$  will have at most  $k$  rows, as required by Algorithm 42.
  4. Delete from  $M$  the first  $c$  rows and columns, obtaining a matrix  $\overline{M}$  of size  $(k-c) \times (n-c)$ .

5. Apply partial spread decoding to  $\text{rowsp}(\overline{M})$  as described in [12], Section 5, and obtain a matrix  $N$  of size  $k - c \times n - c$ .
6. We have  $V^\perp = \text{rowsp} \begin{bmatrix} I_c & 0 \\ 0 & N \end{bmatrix}$ . Use Remark 45 to describe  $V$  as the rowspace of a matrix.

## References

- [1] R. Ahlswede, N. Cai, S.-Y.R. Li, R.W. Yeung, *Network information flow*. IEEE Transactions on Information Theory 46 (2000), 4, pp. 1204 – 1216.
- [2] A. Beutelspacher, *Partial Spreads in Finite Projective Spaces and Partial Designs*. Mathematische Zeitschrift 145 (1975), pp. 211 – 230.
- [3] A. Beutelspacher, *On  $t$ -covers in Finite Projective Spaces*. Journal of Geometry 12 (1979), 1, pp. 10 – 16.
- [4] A. Beutelspacher, J. Eisfeld, J. Müller, *On Sets of Planes in Projective Spaces Intersecting Mutually in One Point*. Geometriae Dedicata 78 (1999), pp. 143-159.
- [5] A. Beutelspacher, U. Rosenbaum, *Projective Geometry: From Foundations to Applications*. Cambridge University Press (1998).
- [6] M. Deza, *Une propriété extrême des plans projectifs finis dans une classe de codes equidistants*. Discrete Mathematics, 6 (1973), pp. 343 – 352.
- [7] M. Deza, P. Frankl, *Every large set of equidistant  $(0, +1, -1)$ -vectors forms a sunflower*. Combinatorica, 1 (1981), pp. 225 – 231.
- [8] D. A. Drake, J. W. Freeman, *Partial  $t$ -spreads and group constructible  $(s, r, \mu)$ -nets*. Journal of Geometry 13 (1979), 2, pp. 210 – 216.
- [9] T. Etzion, N. Raviv, *Equidistant codes in the Grassmannian*. Online preprint: <http://arxiv.org/abs/1308.6231>.
- [10] P. Frankl, R. M. Wilson, *The Erdős-Ko-Rado theorem for vector spaces*. Journal of Combinatorial Theory, Series A, 43 (1986), ppg. 228 –236.
- [11] E. Gorla, F. Manganiello, J. Rosenthal, *An Algebraic Approach for Decoding Spread Codes*. Advances in Mathematics of Communications 6 (2012), 4, pp. 443 – 466.
- [12] E. Gorla, A. Ravagnani, *Partial spreads in random network coding*. Finite Fields and Their Applications, 26 (2014), pp. 104-115.
- [13] T. Ho, M. Médard, R. Kötter, D. R. Karger, M. Effros, J. Shi, and B. Leong, *A random linear network coding approach to multicast*. IEEE Transactions on Information Theory, 52 (2006), pp. 4413-4430.
- [14] R. Kötter, F. R. Kschischang, *Coding for Errors and Erasures in Random Network Coding*. IEEE Transactions on Information Theory, 54 (2008), 8, pp. 3579 – 3591.



- [15] R. Kötter, F. R. Kschischang, D. Silva *A Rank-Metric Approach to Error Control in Random Network Coding*. IEEE Information Theory Workshop on Information Theory for Wireless Networks (2007).
- [16] S.-Y.R. Li, R.W. Yeung, N. Cai, *Linear network coding*. IEEE Transactions on Information Theory, 49 (2003), 2, pp. 371 – 381.
- [17] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*. Cambridge University Press (1986).
- [18] F. Manganiello, E. Gorla, J. Rosenthal, *Spread Codes and Spread Decoding in Network Coding*. IEEE Proceedings (Toronto 2008), pp. 881 – 885.
- [19] M. Médard, A. Sprintson (editors), *Network Coding, Fundamentals and Applications*. Elsevier 2012.
- [20] N. Raviv, T. Etzion, *Distributed Storage Systems based on Equidistant Subspace Codes*. Online preprint: <http://arxiv.org/abs/1406.6170>.